Data Protection Impact Assessment Template: Whistleblowing Channel

A template for the controller. Follows Article 35 GDPR and the EDPB-endorsed WP248rev.01 guidelines. Last updated: 7 November 2026.

---

1. How to use this template

A DPIA is required where processing is likely to result in a high risk to the rights and freedoms of individuals (Article 35(1) GDPR). WP248rev.01, endorsed by the European Data Protection Board, asks for four things in an assessment, and this template is those four things in order: a systematic description of the processing and its purposes (Article 35(7)(a)), an assessment of necessity and proportionality (Article 35(7)(b)), an assessment of the risks to the rights and freedoms of data subjects (Article 35(7)(c)), and the measures that address those risks (Article 35(7)(d)).

The assessment is about risk to the people whose data is processed, not risk to the organisation. A data breach that costs the controller a fine but leaves reporters unharmed is still a risk to them, and a small incident that could identify a single anonymous reporter is a serious one.

- Complete the document before the channel goes live, and update it when the processing changes, not once a year for its own sake.
- Keep the answers, including the ones you decide against. The reasoning is the deliverable.
- Record the advice of the data protection officer separately (Article 35(2)), and the views of data subjects or their representatives where appropriate (Article 35(9)).
- If a high risk remains after the measures, consult the supervisory authority before starting (Article 36(1)).

2. Screening: is a DPIA required?

WP248rev.01 lists nine criteria that indicate high risk. Two or more of them in one processing operation means a DPIA is normally required; one may still require one where the context warrants it. A whistleblowing channel almost always hits more than two, which is why this template exists.

Criterion (WP248rev.01)	In a whistleblowing channel	Applies
Evaluation or scoring, including profiling and predicting	A case assessment can profile a department or an individual, but the tool itself does not score anyone	Partly
Automated decision-making with legal or similarly significant effects	No automated decision is taken about a reporter or a person named in a report	No
Systematic monitoring of a publicly accessible area	The channel is closed and invite-only for handlers; there is no monitoring of reporters	No
Sensitive data or data of a highly personal nature	Allegations of criminal or ethical misconduct, health, sexual harassment, trade union activity; Article 9 and Article 10 GDPR data	Yes
Data processed on a large scale	Depends on headcount and case volume; a channel for a 50-person company is not the same as one for 5,000	Depends
Matching or combining datasets	Cases are stored per organisation and not combined with other datasets by the platform	No
Data concerning vulnerable data subjects	Reporters are vulnerable by definition, and people named in a report may be unaware a case exists	Yes
Innovative use of technology or organisational solutions	On-device dictation and end-to-end encryption are recent, and reduce risk rather than add it	Partly
Preventing data subjects from exercising a right or using a service	Only if access to the channel itself is restricted in a way that blocks a protected disclosure	Depends

Decision for this channel: you complete. Record which criteria you rely on and why, then continue with the four elements below.

Check your own supervisory authority's list before you conclude. Article 35(4) requires every authority to publish the processing operations that need a DPIA, and several national lists name whistleblowing and internal reporting systems explicitly. A mandatory entry there settles the question whatever the screening above says.

3. Description of the processing (Article 35(7)(a))

A systematic description of the processing operations and their purposes, including the legitimate interest pursued where Article 6(1)(f) applies. Describe what happens to a report from the moment it is submitted, in order, and stop at the level of detail a reviewer could check against the system.

Field	What to record
Purpose	Receiving, documenting and following up reports of misconduct, and meeting the internal reporting obligation in the applicable transposition of Directive 2019/1937
Lawful basis	Article 6, and the Article 9 condition for special category content where it appears in a report. Record legal obligation versus legitimate interest, because the two carry different tests
Data subjects	Reporters, people named in a report, witnesses, case handlers, and any third party mentioned in the case file
Data categories	Report content in text, voice transcript or attachment; reporter identity or contact details where given; case notes and status history; handler account and access data
Sources	The reporter, and the case team's own follow-up activity
Recipients	The case handlers the controller designates, and the processor and its sub-processors listed in the processing agreement
Systems and location	The report form, the case dashboard, the database, and the hosting region. Ashio hosts in Vienna, Austria; state whether that is your environment
Retention	The window configured per organisation, when its clock starts, and who deletes expired cases
Transfers	Any processing outside the EEA, and the instrument relied on
Volume	Expected reports per year, and the number of people who can read case data

4. Necessity and proportionality (Article 35(7)(b))

An assessment of whether the processing is necessary for, and proportionate to, the purpose. The question is not whether the channel is useful, it is whether each field, each recipient and each retention day is needed for it.

Question	Evidence to record
Could the purpose be met with less data?	Whether the reporter name is optional, and whether the channel can be offered without collecting it
Is the data accurate and kept current?	How a reporter corrects a statement, and how a case record distinguishes an allegation from a finding
Is the retention limit enforced, not just declared?	The configured window, and proof that expired cases are actually removed, not only marked
Can a data subject exercise their rights?	Access, rectification and erasure for people named in a report, and how a request is balanced against the confidentiality of the reporter
Is the processing transparent to the reporter?	A privacy notice shown before submission, in the reporter's language, naming the recipient and the retention window
Are processor terms in place?	A signed or electronically accepted processing agreement, a sub-processor list, and the objection route

Ashio provides: a reporter-facing privacy notice generated from the organisation's own settings, an optional reporter name field, anonymity as the default path, and a processing agreement that is accepted electronically and downloadable as a PDF.

5. Risks to the rights and freedoms (Article 35(7)(c))

WP248rev.01 expresses risk as a combination of likelihood and severity, judged from the data subject's point of view. The rows below are the risks a whistleblowing channel actually produces. Record likelihood, severity and the resulting risk for each row before the measures, then again after them, and say how you scored it.

Risk	Cause	Impact on the data subject
A reporter is identified	Weak anonymity, device metadata, a filename, a distinctive writing style, or a small team where an incident is recognisable	Retaliation, dismissal, criminal exposure
Case content is read by someone who should not see it	Over-broad handler access, a shared login, a forwarded PDF, a misdirected invitation	Exposure of an allegation against a person who may be innocent
A person named in a report is harmed by a premature disclosure	Notification before verification, or disclosure to the subject of the allegation	Reputational and professional damage from an unproven allegation
A special category is inferred	Health, sexual harassment or union activity in the narrative, even where not asked for	Article 9 exposure and discrimination
Data is kept longer than needed	A retention window that is declared but not enforced	Prolonged exposure and stale, unproven allegations
A transfer lacks a valid instrument	A sub-processor outside the EEA without standard clauses	Loss of the protection the data subject is entitled to expect
The reporter cannot exercise their rights	No way to ask what is held, or a request answered by the employer rather than the controller	Loss of control over their own statement

Ashio reduces several of these by design: report bodies, messages and attachments are encrypted in the reporter's browser, so the server holds ciphertext it cannot read; the report page collects no IP address and sets no cookies; and attachments are stripped of location, camera and author metadata before encryption. Those are properties of the tool, not a conclusion of your assessment. Assess them, do not copy them.

6. Measures and residual risk (Article 35(7)(d))

6.1 Measures

Measure	Type	Status
End-to-end encryption of report bodies, messages and attachments	Technical	Provided by Ashio
Anonymity available by default, with no IP address or cookies on the report page	Technical	Provided by Ashio
Role-based access limited to the case team, with per-case assignment	Organisational and technical	You configure
Append-only case history, exported as PDF when needed	Technical	Provided by Ashio
Retention window per organisation, published in the reporter notice	Organisational	You decide and you verify deletion
Sub-processor list with a 30-day notice and an objection route	Contractual	Provided by Ashio
Hosting in Vienna, Austria, inside the EEA	Contractual and technical	Provided by Ashio
Handler training, confidentiality undertakings and access reviews	Organisational	You provide
A route for a person named in a report to exercise their rights	Organisational	You provide

6.2 Advice and consultation

- Data protection officer: record the advice given, the date, and whether it was followed (Article 35(2)). If it was not followed, say why.
- Data subjects or their representatives: record whether their views were sought, and how (Article 35(9)). A works council or staff representatives are the usual route for a reporting channel.
- Residual risk: for each row in section 5, record the score after the measures and whether it is acceptable.
- Prior consultation: if a high risk remains, the supervisory authority must be consulted before processing begins (Article 36(1)). Name the authority and the date of the consultation.

6.3 Sign-off

Role	Name	Date
Controller, accountable for the assessment	You complete	You complete
Data protection officer, advice recorded	You complete	You complete
Processor contact, for the technical description	Ashio, legal@ashio.eu	You complete
Review date, or the trigger for a new assessment	You complete	You complete

7. What Ashio provides, and what stays with you

A processor can supply the technical facts and the contractual instruments. It cannot supply the lawful basis, the sign-off, or the operational discipline, because those belong to the controller. The split, so that this template is not mistaken for a completed assessment:

- Ashio provides: the encryption design, the anonymity defaults, the access model, the audit trail, the retention setting, the processing agreement, the sub-processor annex and this template.
- You provide: the lawful basis, the necessity analysis, the risk scores, the DPO's advice, the views of data subjects, the sign-off, the handler training, the access reviews, and the check that expired cases are actually deleted.
- You remain the controller. Nothing in this document transfers a controller obligation to Ashio, and nothing in it is legal advice.

8. Sources

- Article 29 Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is likely to result in a high risk for the purposes of Regulation 2016/679, WP248rev.01, endorsed by the European Data Protection Board on 25 May 2018: ec.europa.eu
- Regulation (EU) 2016/679, Articles 35 and 36: eur-lex.europa.eu
- Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law: eur-lex.europa.eu